AFFIDAVIT OF SPECIAL AGENT IAN D. SMYTHE IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT AND A CRIMINAL COMPLAINT

I, IAN D. SMYTHE, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the FBI since June 29, 2003 and am currently assigned to the Boston Field Office, Springfield Resident Agency. I have been involved in investigations related to the sexual exploitation of children since approximately June of 2004. Since joining the FBI, I have investigated violations of federal law, and currently investigate federal violations concerning child pornography and the sexual exploitation of children, as well as civil rights violations, public corruption, health care fraud violations, and other complex white collar crimes. I have gained experience through training in seminars, classes, and everyday work related to conducting these types of investigations. I have been involved in multiple investigations involving sex crimes against children, to include leading investigations related to the sexual exploitation of children and child pornography, writing and executing search warrants, interviewing victims, interviewing suspects and conducting arrests.
2. Prior to employment with the FBI, I was employed for approximately 12 years as a United States Army officer in the areas of intelligence and special operations.
3. I am currently investigating Ronald S. Brown ("Brown"), of , Williamstown, Massachusetts, for violating Title 18, United States Code, Sections 2251 (Sexual Exploitation Of Minors), 2252(a)(2) (Receipt Of Material Involving The Sexual

Exploitation Of Minors), 2252(a)(4)(B) (Possession Of Material Involving The Sexual Exploitation Of Minors, 2252A(a)(2) (Receipt Of Child Pornography), 2252A(a)(5)(B) (Possession Of Child Pornography), 2422(b) (Enticement Of A Minor To Engage In Criminal Sexual Activity), and 2423(a) (Transportation Of A Minor With Intent To Engage In Criminal Sexual Activity) (the "Subject Offenses").

4. I submit this affidavit in support of an application for warrants under 18 U.S.C. § §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Rule 41 of the Federal Rules of Criminal Procedure to search and seize a Facebook account with the user identification of ronnie.brown.01267 (the "Subject Facebook Account"), a Yahoo Messenger account in the name of energizer2758@yahoo.com (the "Subject Yahoo Account"), an e-mail account in the name of rabbit2758@gmail.com (the "Subject Gmail Account"), and an e-mail account in the name of rabbit2758@msn.com (the "Subject MSN Account"), other user-generated data associated with these accounts, and associated subscriber, transactional, and user connection information associated with these accounts, as described in Attachments A and B. The Subject Accounts are relevant to the investigation because there is probable cause to believe that between on or about December 23, 2012 and on or about January 19, 2013, Brown used the Subject Accounts to produce, solicit, and/or receive child pornography featuring a sixteen year-old minor male ("Minor A") and to arrange for Minor A to travel to New Jersey and New York for the purpose of meeting Brown and engaging in illicit sexual conduct with him. I therefore have probable cause to believe that these accounts contain evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachment B. Based on the

information provided by Facebook, Yahoo, Google, and Microsoft, I have probable cause to believe that the accounts and relevant data are maintained by Facebook, Yahoo, Google, and Microsoft, respectively, which accept service of process as described in Attachment A at:

a. Facebook, Inc.
Security Department/Custodian of Records,
156 University Avenue, Palo Alto, CA 94301
Fax: 650-644-3229

b. Yahoo! Inc.
Custodian of Records
Attn: Compliance Team,
701 First Avenue, Sunnyvale, CA 94089,
Fax : 408-349-7941

c. Google, Inc.
Attention: Custodian of Records
1600 Amphitheatre Parkway
Mountain View, CA 94043
Fax: 650-649-2939

d. Microsoft Corporation
Attn: MSN Custodian of Records
One Microsoft Way, Redmond, WA 98052
Fax: 425-727-3490

5. I also submit this affidavit in support of an application Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following locations and items, as described in Attachment A, because there is probable cause to believe they contain evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachment B:

a. Brown's residence, located at , Williamstown, Massachusetts (the "Subject Residence");

b. Brown's vehicle, a blue, 2008, four-door Dodge Ram Quad Pickup with MA license plate No. 69YN86 (the "Subject Vehicle")

c. Brown's laptop computer, a Sony VAIO laptop computer with serial number C6021UER (the "Subject Laptop"); and

d. Brown's cellular telephone, an HTC Incredible cellular telephone with serial number HT26J310727 (the "Subject Cell Phone").

6. I am also submitting this Affidavit in support of a Criminal Complaint alleging that in or about January 2013, the defendant committed a violation of Title 18, United States Code, Section 2251, to wit, the defendant used, persuaded, induced, and enticed, Minor A to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct and for the purpose of transmitting a live visual depiction of such conduct, knowing and having reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents, investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search and arrest warrants and does not set forth all of my knowledge about this matter.

RELEVANT STATUTES

8. Title 18, United States Code, Section 2251(a) provides in pertinent part:

> Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

18 U.S.C. § 2251(a).

9. Title 18, United States Code, Section 2252(a)(2) provides in pertinent part:

> Any person who . . . (2) knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, . . . if –
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
> (B) such visual depiction is of such conduct;
>
> . . . shall be punished . . . .

18 U.S.C. § 2252(a)(2).

10. Title 18, United States Code, Section 2252(a)(4)(B), provides in pertinent part:

> Any person who . . . knowingly possesses or knowingly accesses with intent to view 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if –
>
> (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (ii) such visual depiction is of such conduct;
>
> . . . shall be punished . . . .

18 U.S.C. § 2252(a)(4)(B).

11. Title 18, United States Code, Section 2252A(a)(2) provides in pertinent part:

> [a]ny person who -
>
> (2) knowingly receives or distributes -
>
> (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or
>
> (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;
>
> shall be punished as provided . . . .

18 U.S.C. § 2252A(a)(2).

12. Title 18, United States Code, Section 2252A(a)(5)(B) provides in pertinent part:

> [a]ny person who –

> (5)(B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; . . .
>
> shall be punished as provided . . . .

18 U.S.C. § 2252A(a)(5)(B).

13. The term "computer" as used herein is defined in Title 18, United States Code, Section 1030(e)(1), as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1).

14. Title 18, United States Code, Section 2256(1) defines a "minor" as "any person under the age of eighteen years." 18 U.S.C. § 2256(1).

15. Title 18, United States Code, Section 2256(2)(A) defines "sexually explicit conduct" as "actual or simulated -- (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii)

masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." 18 U.S.C. § 2256(2)(A).

16. Title 18, United States Code, Section 2256(5) provides that "visual depiction" includes "undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format." 18 U.S.C. § 2256(5).

17. Title 18, United States Code, Section 2256(8) defines "child pornography" in pertinent part:

> [A]ny visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where –
>
> (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
>
> (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
>
> (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 U.S.C. § 2256(8).

18. Title 18, United States Code, Section 2422(b) provides in pertinent part: "Whoever, using the mail or any facility or means of interstate or foreign commerce . . . knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years , to engage in . . . any sexual activity for which any person can be charged with a criminal

offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life." 18 U.S.C. § 2422(b).

19. Title 18, United States Code, Section 2423(a) provides in pertinent part: "A person who knowingly transports an individual who has not attained the age of 18 years in interstate . . . commerce . . . with intent that the individual engage in . . . any sexual activity for which any person can be charged with a criminal offense, shall be fined under this title and imprisoned not less than 10 years or for life." 18 U.S.C. § 2423(a).

20. Section 130.40.2 of the New York Penal Law (Criminal Sexual Act In The Third Degree) provides in pertinent part: "A person is guilty of criminal sexual act in the third degree when: . . . Being twenty-one years old or more, he or she engages in oral sexual conduct or anal sexual conduct with a person less than seventeen years old." N.Y. Penal Law § 130.40.2. Criminal sexual act in the third degree is a class E felony. Id.

21. Section 130.05.1 of the New York Penal Law (Sex Offenses; Lack Of Consent) provides in pertinent part: "Whether or not specifically stated, it is an element of every offense defined in this article that the sexual act was committed without consent of the victim." N.Y. Penal Law § 130.05.1. Section 130.05.2(b) provides in pertinent part : "Lack of consent results from . . . [i]ncapacity to consent . . . ." N.Y. Penal Law § 130.05.2(b). Section 130.05.3(a) provides in pertinent part: "A person is deemed incapable of consent when he or she is . . . less than seventeen years old . . . ." N.Y. Penal Law § 130.05.3(a).

DEFINITIONS

22. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

23. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); United States v. Caldwell, No. 97 5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

24. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

25. A "hash value" is the result of a calculation (i.e., a hash algorithm) performed on a data input (e.g., a string of text, an electronic file, or the entire contents of a hard drive). Hash values are used to identify duplicate files or verify that a forensic image was captured successfully. One common hash value is known as Secure Hash Algorithm Version 1 ("SHA-1"). Two files with the same SHA-1 value are identical to a degree of precision greater than 99.99999 certainty. I am unaware of any documented occurrence in which two files have the same content but different SHA-1 values.

26. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device.

27. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

28. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. The IP address provides a unique location for that computer, making it possible for that computer to participate in data transfers over the Internet with other computers. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to the user's computer every time it accesses the Internet. IP addresses can also be static, meaning that the ISP assigns the user's computer a particular IP address that is used each time the computer accesses the Internet.

29. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first-level or top-level domains are typically .com for commercial organizations, .gov for governmental entities, .org for non-commercial organizations, and, .edu for educational entities and institutions. Second-level names will further identify the organization, and additional levels may exist as needed.

30. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

31. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

32. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

33. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

34. "Globally Unique Identifier" or "GUID" refers to the unique identification of the individual installation of peer-to-peer ("P2P") software on an individual computer. Law enforcement authorities can use the GUID to identify a specific computer even if the IP has changed.

35. The terms ".jpeg," ".jpg," ".gif," ".bmp", and ".tiff" are file extensions which typically denote graphic image files.

36. The terms ".mpeg," ".mpg," ".mov," ".avi," ".rm," and ".wmv" are file extensions which typically denote video image files. To use these video files, one needs a personal computer with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

Background Regarding Child Pornography, Computers, And The Internet

37. I have been formally trained in the investigation of crimes involving the sexual exploitation of children and have participated in numerous such investigations. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet for many years. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

a. Child pornographers in the past could possess an actual hard copy photograph and transfer these photographs onto a computer-readable format through the use of a scanner. With the advent of digital cameras, the images can now be transferred directly from the camera onto a computer. A device known as a modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Electronic contact can thus be made to literally millions of computers around the world. The ability to use computers to produce child pornography easily, reproduce it inexpensively, distribute it anonymously (through electronic communications), and store it in large quantities has drastically changed the method of possession, receipt, distribution, and production of child pornography. Child pornography can now be transferred via electronic mail or through file transfer protocols ("FTP") to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail services, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is the preferred method of committing the Subject Offenses.

b. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk, compact disk, or thumb drive can store hundreds of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime" (i.e., the physical location of the computer). Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail and identify the remote storage location.

c. With Internet access, a computer user can transport an image file from the Internet or from another user's computer, so that the image file is stored on their computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printing device (such as a laser or inkjet printer).

d. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via

the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The computer's Internet browsing software typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

38. Even if there were an open, unsecure wireless access point ("WAP") at the Subject Premises, it would not tend to defeat probable cause. See United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007). If someone outside of the Subject Premises were using an open, unsecure WAP inside the Subject Premises, there would still be probable cause to believe that the

Subject Premises will contain evidence because the WAP itself and any logs kept by the WAP would be evidence. Also, even if the Subject Premises contained an open, unsecure WAP, I believe based upon my training and experience that there would still be probable cause to believe that the person using a computer at the Subject Premises described above to access child pornography electronically was doing so inside the Subject Premises for a number of reasons, including accessibility, ease of communication, and the need for privacy when accessing child pornography.

Characteristics of Child Sex Offenders

39. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive child pornography are often individuals who have a sexual interest in children and in sexual depictions of children, and that there are certain characteristics common to such individuals:

40. Individuals who have a sexual interest in children or sexual depictions of children may receive sexual gratification, stimulation, and satisfaction from direct physical contact with children; from fantasies they may have after or while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

    a. Individuals who have a sexual interest in children or sexual depictions of children may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings or other

visual media. Individuals who have a sexual interest in children or sexual depictions of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

b. Individuals who have a sexual interest in children or sexual depictions of children almost always possess and maintain their "hard copies" of child pornographic media in the privacy and security of their home or some other secure location. These individuals often maintain their "hard copy" collections for many years.

c. Likewise, individuals who have a sexual interest in children or sexual depictions of children often maintain their digital or electronic collections in the privacy and security of their home or some other secure location. These individual often maintain their digital or electronic collections for many years.

d. Individuals who have a sexual interest in children or sexual depictions of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or sexual depictions of children prefer not to be without their child pornography for any prolonged time period, and access their collections frequently.

Brown's Criminal History

41. According to Brown's criminal history report, on March 24, 1995, Brown was convicted and sentenced for three crimes in two separate Connecticut cases:

a. Brown was convicted in Litchfield Judicial District Court Docket No. CR94-83667 of one count of sexual assault in the second degree in violation of Conn. Gen. Stat. Section 53a-71 and sentenced to ten years in jail with five years to serve and five years of probation, and of one count of delivering liquor to a minor in violation of Conn. Gen. Stat. Section 30-86 and sentenced to one year in jail (suspended and concurrent) and two years of probation.

b. Brown was convicted and sentenced in Litchfield Judicial District Court Docket No. CR94-84537 with one count of tampering with a witness and was sentenced to three years in jail (suspended and concurrent).

42. According to records of the Connecticut Judicial Department, Office of Adult Probation, between August 23 to 26, 1994, Brown had sexually assaulted a twelve year-old minor male at a campground in North Canaan, Connecticut after providing him liquor. According to the minor's complaint, while the minor was sleeping in their tent, Brown pulled down the minor's shorts and underpants and inserted his finger into the boy's anus and then threatened

him by saying "if you tell anyone I'll come get you. I know where you live." In a later incident, Brown threw the boy to the ground and grabbed his penis; according to a subsequent medical examination, the boy had abrasions on his penis and cuts on his shins and hands. On approximately December 6, 1994, Brown called the boy and stated "I'm going to kill you, you're a dead motherfucker." The defendant entered pleas of *nolo contendere* to his offenses of conviction.

43. Brown is currently 50 years old and a registered Level 2 sex offender.

The Instant Investigation Of Brown's Commission Of The Subject Offenses

44. According to the Massachusetts Registry of Motor Vehicles ("MA RMV"), Brown's address is the Subject Premises (no apartment number) and is the registered owner of the Subject Vehicle.

45. According to a Williamstown Police Department ("WPD") Incident Report filed by WPD Sgt. Scott McGowan, on the afternoon of January 19, 2013, the mother of Minor A, who resides with Minor A in , reported that Minor A was missing and believed to be in Williamstown, Massachusetts. Minor A's mother stated that after she discovered Minor A missing from her house, she located a Skype account on a laptop computer at her house that contained extremely sexual communications between Minor A and "Ronnie Brown" of Williamstown. According to Minor A's mother, Brown and Minor A were also "friends" on Facebook.

46. According to Minor A's mother, in one message, Minor A told Brown that he needed to use the bathroom, and Brown responded that he wished he was with Minor A so that he could

hold Minor A's penis. In another message, Minor A told Brown that he needed to take a shower, and Brown responded that it would be the last time that Minor A would shower alone. Minor A's mother also read material suggesting that Minor A flew from to an East Coast location earlier on the morning of January 19, 2013.

47. Based upon the report by Minor A's mother, WPD officers responded to the Subject Residence, but could not locate the Subject Vehicle, which Brown was known to operate. Sgt. McGowan left a telephone message with Brown, requesting a return call. Later in the afternoon, Brown returned Sgt. McGowan's call, and told Sgt. McGowan that he was traveling northbound on the New York Thruway with Minor A en route to the Subject Residence. Sgt. McGowan directed Brown to pull his vehicle to the roadside and activate his emergency four-way flashers, explaining that Minor A was sixteen years old and had been reported as a missing juvenile who needed to be returned home to . Brown agreed to stop.

48. According to New York State Police ("NYSP") Trooper David Rose, he and Trooper Christopher Baldner encountered Brown and Minor A in the Subject Vehicle on the side of the New York Thruway at Mile Marker 80 Northbound. Trooper Baldner transported Minor A to the NYSP's Highland Barracks, and Brown voluntarily followed them in the Subject Vehicle. Brown subsequently left the area in the Subject Vehicle.

49. At approximately 9:00p.m. on January 19, 2013, I and Supervisory Special Agent Mark Karengekis arrived at the Kingston DPW facility, on the New York Thruway, where we assumed custody of Minor A and transported him to the Williamstown PD. I and Massachusetts State Police ("MSP")

Trooper Michael Scott then conducted an interview of Minor A, who subsequently executed a written statement that stated, among other things:

a. Minor A is sixteen years old and sexually interested in older men.

b. On December 23, 2012, Minor A logged onto a chat room at Silverdaddies.com (using the username and the false age of eighteen), and began chatting with Brown.

c. Brown and Minor A also communicated via Yahoo Messenger, and Minor A used the e-mail account @yahoo.com. Brown and Minor A also were friends on Facebook, on which Minor A listed his correct age.

d. In a Yahoo Messenger chat dated December 27, 2012, Minor A told Brown that he was 16 years old, and Brown responded that this age did not bother him.

e. On approximately January 3, 2013, Brown's conversations with Minor A began to be sexual in nature. After their conversations became sexual, Minor A and Brown began communicating by Skype.

f. On January 8, 2013, Brown and Minor A communicated by Skype, during which Minor A masturbated for Brown through a video chat. During this chat, Brown told Minor A that he wanted to "fuck me."

g. On January 13, 2013, Brown and Minor A communicated by Skype, during which Minor A displayed his penis to Brown. Later that day during another video chat, Brown displayed his penis and buttocks to Minor A.

h. In the beginning of January, Brown and Minor A arranged for Minor A to live with Brown in Massachusetts. Brown purchased a plane ticket for Minor A and mailed him $150 for a taxicab and for food at the airport.

i. On January 19, Minor A flew on Southwest Airlines to Newark, New Jersey and met Brown at the airport. Brown then began to drive Minor A in a four-door blue Dodge pickup truck (which I believe to be a description of the Subject Vehicle) toward Brown's residence in Williamstown (which I believe to be the Subject Residence), where they intended to have anal sex. Brown had a digital camera in the vehicle, but Brown did not take any photographs of Minor A.

50. Also on January 19, 2013, Minor A permitted me to access his Yahoo Messenger, FaceBook, and Silverdaddies.com accounts. That evening, I reviewed these accounts and located numerous online communications between Brown and Minor A.

51. Minor A's Facebook account included a link to Brown's Facebook account, which included numerous photographs of Brown and the user identification of ronnie.brown.01267 (i.e., the Subject Facebook Account).

52. According to my review of Minor A's Yahoo Messenger account, Brown used the following username: energizer2758 (i.e., the Subject Yahoo Account).

53. On or about December 27, 2012, Minor A engaged in a Yahoo Messenger chat with Brown, in which Minor A informed Brown that he was sixteen years old:

11:26:10 PM :
well, before that there is one thing i have to tell you

11:26:43 PM Ron Brown:
And that is? don't worry, you can tell me anything

11:32:01 PM :
I'm 16, 17 in february. I'm sorry for lying to you, but 1 is the only way to make a profile and 2 it's one of the only ways to get people to take me seriously. I've really enjoyed this conversation, and hope we can keep talking, but i feel terrible for lying to you like that. Besides that, i've been completely honest with you. If you're worried about legal ramifications or the like. Just know that 16 is the age of consent where i'm at so you can't get in any trouble for what we talked about. Nor am i the kind of scum that would share this for "bragging rights

11:32:14 PM
i'm sorry

11:33:49 PM Ron Brown:
First, I appreciate the honesty. Second, 16 is legal here, too. I do understand ... and we will definitelyl continue, I'm not letting you go that easily, ... I wish I could hug you right now to show you how I feel .. your honesty shows me even more that you're serious and real .. not playing games ... does make me wonder , about your living situation and 'availability' ... but that's only because I do want to continue

54. On December 28, 2013, Minor A and Brown engaged in the following chat on Yahoo Messenger, in which I believe, based upon my training, experience, and knowledge of the case, Brown accepted Minor A's request to communicate with him through Skype:

1:36:51 AM

do you have a skype?

1:39:22 AM Ron Brown:
I do indeed, ronnie2759

1:39:33 AM Ron Brown:
Correction ronnie2758

1:40:43 AM :
one sec

1:41:09 AM Ron Brown:
K

1:44:57 AM :
request away

1:45:21 AM Ron Brown:
Request accepted

55. On January 1, 2013, Minor A and Brown engaged in the following chat on Yahoo Messenger:

12:16:46 AM Ron Brown:
I just started perusing ... and I'm debating telling you the two ways I wanted to start 2013 ths minute

12:17:23 AM :
i want to hear them

12:17:59 AM Ron Brown:
What if you laugh, or at least snicker? LOL One is 'x' and one is 'g'

12:18:41 AM :
i still want to hear them both

12:19:06 AM Ron Brown:
okay, which first, X or G

12:19:52 AM :
tell them both at the same time

12:20:47 AM Ron Brown:
The "X" is right now for you to be naked, sitting on my face, grinding your cute, sweet, very tight ass down into my face as my tongue works up into you ... the "G" and I think better one is

that you and I are laying in bed, curled up together kissing deeply and snuggling

56. On January 3, 2013, Brown sent Minor A the following text on Facebook: "Good afternoon, Squishy! Thank you so much for friending me. Do you have any idea what it means to me? HUGS KISSES HUGS KISSES, TUGS GROPES HUGS KISSES."

57. On January 5, 2013, Brown and Minor A engaged in the following text exchange on Facebook:

Brown:
so MUCH of you to eat, gonna make it my full time job... and I had a very SEXUAL, thought, this morning when I woke up not 'physical' exactly, but soimething you could 'brag' about.

Minor A:
oh?

Brown:
yah.. you might be the only HS student to have a sex life like this, not having to go FIND it, or worry about a GF/BF and able to get laid every single morning before school... HOT?

58. On January 10, 2103, Brown and Minor A engaged in the following text exchange on Facebook:

Minor A:
lol, i was just kidding about the gems

Brown:
what, someone sent you some?

Minor A:
yeah, some 50 year old

Brown:
WTF he's DEAD! How dare he try and steal you away! LOL

Minor A:
between you and me he's kinda ccute, though i think he just wants to get in my pants

Brown:
will he fit in your pants?

Minor A:
Definitely

Brown:
well, I guess the big question is, do you want that guy in your pants and what do you want him to do when he gets in them

Minor A:
yeah, i'd get him on his knees and shove my cock down his throat and use his spit to fuck him hard, spew my load in his ass. for starters sit on his face and have him rim me for a while

Brown:
hmmm well, I know I sure would want that... but you gotta fuck his face HARD, then tear his ass up, and make him rim you for at least an hour until you cum without touching yourself, or have him do it as he rims you

Minor A:
i plan on it, and the last part is something i will have to try

Brown:
mmmm grind that ass in to his face... hey, if we keep this up, 's pants are gonna get really tight and he's gonna have to go skype in the bathroom... or one can only hope LOL

Minor A:
i'm saving it for you on the 19th
Brown:

you think you can go another 8 days, babe? That's kind of rough for you I think, but then again, yo have the most amazing self control,

59. On January 13, 2013, Brown and Minor A engaged in the following text exchange on Facebook:

Brown:
LOL But what is the first thing I want to do with you, besides the incredible airport greeting, like when we get to your home

Minor A:
fuck like rabbits

Brown:
LOL I wouldn't complain about that but I have something else even more on my mind
stumped?

Minor A:
just a litte

Brown:
cuddle/snuggle, of course, that will most likely lead to our bunny impersonation

Minor A:
Lol

Brown:
of course, that may all be academic after spending a few hours with you in the car, we may not make it past the front door/dining room table... but since you're in charge, I leave that up to you
if we go right to the bunny act, you're likely to think I did all this to get one thing

Minor A:

i could sit in the driver's seat and have you ride my dick all the way to your house our

Brown:
mmmm love the correction, and that would work,, I'll find a bumpy road to do all the... 'work'

Minor A:
i'm game

Brown:
I wonder what you would do if as soon as we get in the Ram, you moved to the center so I could hold you and then if you would move my hand to a certain location?

Minor A:
that'd be good too, though the other idea is breaking my resolve

Brown:
LOL As for your resolve, you have 140 plus hours so I said last night if you wanted to do something on skype, I'd be good, I don't want you um... suffering
how long before you might 'move my hand' in the truck? LOL

Minor A:
Lol

Brown:
to which?

Minor A:
almost immediately

Brown:
I can work with that, besides the truck is an automatic... as for the resolve, I support you in whatever you decide...

60. Minor A's Yahoo e-mail account contained a folder entitled "Ron Brown," and included e-mails exchanged between Minor A and Brown.

61. For example, on January 15, 2013, Brown used the e-mail address rabbit2758@msn.com (i.e., the Subject MSN Account) to send Minor A an e-mail at @yahoo.com entitled ""To do" list – UPDATED TUESDAY . . . . URGENT." This e-mail includes the following items:

    a. "1. Call Taxi company, find out roughly what it's going to cost from your 'neighborhood', [give a cross street, don't have them pick up up right at your house..."

    b. "4. Before you leave, and it might take a little while, wipe your profile off the laptop, please."

    c. "9. Start bringing home, Friday at the latest, ALL your 'pesronal stuff' from your locker and school."

62. Similarly, on January 16, 2013, Brown used the e-mail address rabbit2758@msn.com to send Minor A an e-mail at @yahoo.com entitled "Fw: Your trip is around the corner!"). The e-mail contains a one-way flight itinerary for Minor A, from to Newark, New Jersey.

63. On January 16, 2013, Brown sent Minor A the following text message on Facebook: "make you a deal. if we can skype, I'll be shirtless and any time [the first initial of Minor A's brother] is not around, show you anything you want..."

64. On January 19, 2013, at approximately 10:27 p.m., WPD officer Tania Hernandez reported that Brown had returned to the Subject Residence. Soon thereafter, Sgt. McGowan and MSP Trooper Matthew Boyer arrived at the Subject Residence and met Brown, who agreed to speak to them at the WPD station.

65. At approximately 10:57 p.m., Brown arrived at the WPD Station. At approximately 12:01 p.m. on January 20, 2103, Brown executed a written Miranda waiver, which stated that he wished to speak with the police. In a consensually video recorded interview, Brown then stated, among other things, that:

    a. In late December, Brown met Minor A through the silverdaddies.com website.

    b. Brown exchanged nude photos with Minor A through texts. Approximately a couple weeks earlier, Minor A texted a nude photo of himself, which Brown received on his cell phone (i.e., the Subject Cell Phone) and then forwarded to his computer (i.e., the Subject Laptop) to a folder titled "[Minor A's initials]." Brown initially denied that he requested Minor A's nude photo, but then stated that he "wasn't sure" whether he asked for the photo. Brown insisted (falsely) that he didn't know that Minor A was sixteen at the time that Minor A sent him his nude photo and that because Brown thought Minor A was eighteen, he did not consider the nudity to "be a problem."

    c. Brown had a Skype account.

66. At approximately 12:49 a.m., Brown executed a MSP "Consent To Search" Form, in which he consented to a search of a "Sony Laptop VAIO" (i.e., the Subject Laptop) and an "HTC Incredible" cellular telephone (i.e., the Subject Cell Phone). At approximately 12:51 a.m.,

Brown executed a "Consent To Search Computer Equipment / Electronic Data" form for the Subject Laptop and the Subject Cell Phone.

67. At approximately 1:25 a.m. on January 20, 2013, Sgt. McGowan and Trooper Boyer followed Brown to the Subject Residence, where Brown provided them with the Subject Laptop and the Subject Cell Phone.

68. At approximately 1:52 a.m. on January 20, 2013, at the Subject Residence, Supervisory Special Agent Mark Karengekis and Trooper Boyer recontacted Brown. They reminded Brown of his earlier *Miranda* waiver, advising that he had previously waived his *Miranda* rights and agreed to speak with investigators, reiterated that Brown was not in custody, and asked if they could speak with him again. Brown agreed to speak with investigators and invited them inside the Subject Residence. In an audio-recorded interview, Brown stated, among other things, that:

a. Brown used the Yahoo Messenger identification of "energizer2758" (i.e., the Subject Yahoo Account).

b. Brown thought Minor A was eighteen. However, after Brown was shown a print-out of a Yahoo! Messenger chat in which Minor A informed Brown that he was only sixteen, Brown admitted that in late December 2012, he knew Minor A was sixteen. Brown explained that he lied to law enforcement investigators in order to protect both Minor A and himself.

c. When Brown was confronted with Minor A's claims that Minor A and Brown engaged in sexually explicit conduct over Skype, Brown stated "that happened" and

he was "not denying it." When Brown was asked if he and Minor A masturbated together over Skype, Brown indicated in the affirmative. When Brown was asked if he requested Minor A to masturbate for him on Skype, Brown indicated in the affirmative.

d. When Brown was asked if his chats and Skype sessions with Minor A were an effort to ensure that Minor A was committed to him, Brown responded that "we were already committed to each other."

69. On or about January 20 and 22, 2013, I conducted a preliminary forensic examination of the Subject Laptop and discovered, among other things, the following items:

a. One image of Minor A naked and holding his penis for the camera. A copy of this image is attached as Exhibit 1. According to my preliminary forensic examination, this photo was created on or about January 8, 2013.

b. Multiple additional images and videos depicting young males, whose ages and identities remain unknown at this time, in nude, semi-nude, and sexually provocative positions. Based on my training and experience, I believe these images may constitute child pornography.

70. On or about January 29 and 30, 2013, I conducted a preliminary forensic examination of the Subject Cell Phone and discovered, among other things, a gmail.com e-mail account with e-mail address rabbit2758@gmail.com (i.e., the Subject Gmail Account), that Brown had used to exchange numerous e-mail messages with Minor A's e-mail account, @yahoo.com. In one of these e-mails, Brown forwarded a Southwest Airlines travel

itinerary for Minor A to travel to Newark, New Jersey, to meet with Brown. I also discovered numerous text messages exchanged between Minor A, whom Brown referred to as "Squishy," and Brown, such as the following:

a. "Squishy" 01/18/13 18:51:40 (GMT-5) Incoming: I love you too

b. "Squishy" 01/18/13 18:52:51 (GMT-5) Outgoing: I bet you 1,000,000 1,000,000,000 1,000,000,000,000 quadrillion gazillion Infiniti dollars that I love you more

c. "Squishy" 01/18/13 18:58:54 (GMT-5) Incoming: Pay up :P

d. "Squishy" 01/18/13 18:59:18 (GMT-5) Outgoing: Come and get it

e. "Squishy" 01/18/13 19:56:06 (GMT-5) Outgoing: I will be there tomorrow and I will send you pictures from the road if you want when you send me the picture from the airplane. :-* I love you!!!!!!!!!!!!! <3

71. On January 29, 2013, an FBI forensic interviewer conducted a consensually recorded interview with Minor A in . According to the forensic interviewer, Minor A stated that he and Brown engaged in sexual acts in New York State, while en route from Newark to Massachusetts, including mutual masturbation and/or oral sex. I have requested, but not yet received, a copy of the recording of this interview from the FBI's Office.

PROBABLE CAUSE TO BELIEVE THAT THE ITEMS TO BE SEARCHED CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES OF THE SUBJECT OFFENSES

72. As set forth above, Brown used the Subject Facebook Account to exchange numerous communications with Minor A concerning sexually explicit conduct and Minor A's trip from

to Massachusetts. Therefore, I expect that the Subject Facebook Account will contain evidence, fruits, and instrumentalities of the Subject Offenses.

73. As set forth above, Brown used the Subject Yahoo Account to exchange numerous text messages with Minor A concerning sexually explicit conduct and Minor A's trip from (to Massachusetts and to arrange Skype access with Minor A. Therefore, I expect that the Subject Facebook account will contain evidence, fruits, and instrumentalities of the Subject Offenses.

74. As set forth above, Brown used the Subject Gmail Account to exchange numerous text messages with Minor A concerning sexually explicit conduct and Minor A's trip from to Massachusetts and to discuss Skype communication with Minor A. Therefore, I expect that the Subject Facebook account will contain evidence, fruits, and instrumentalities of the Subject Offenses.

75. As set forth above, Brown used the Subject MSN Account to exchange e-mails with Minor A concerning Minor A's trip from to Massachusetts. Therefore, I expect that the Subject Facebook account will contain evidence, fruits, and instrumentalities of the Subject Offenses.

76. As set forth above, Brown lived at the Subject Residence and arranged for Minor A to travel to from to the Subject Residence, where he expected Minor A to reside with him as a sexual partner. Brown also retrieved the Subject Cell Phone and the Subject Laptop from the Subject Residence. Therefore, I expect that the Subject Residence will contain evidence, fruits, and instrumentalities of the Subject Offenses.

77. As set forth above, Brown admitted that he received a nude photo of Minor A on the Subject Cell Phone and forwarded this photo to the Subject Laptop. In addition, I conducted a preliminary forensic examination of the Subject Laptop and discovered an image of Minor A naked and holding his penis for the camera, as well as other image and video files that I believe may constitute child pornography. Further, I conducted a preliminary forensic examination of the Subject Cell Phone and discovered, among other things, that Brown had used the Subject Gmail Account to exchange numerous e-mail messages and/or text messages with Minor A concerning, among other things, Minor A's travel from o New Jersey. Lastly, according to my preliminary forensic examinations, both the Subject Cell Phone and the Subject Laptop contained the Skype application installed on the devices. Thus, I expect that the Subject Laptop and the Subject Cell Phone will contain evidence, fruits, and instrumentalities of the Subject Offenses.

78. As set forth above, on January 19, 2013, Brown used the Subject Vehicle to pick up Minor A at an airport in Newark, New Jersey and transport him through New Jersey and New York, with the intent to engage in sexual conduct with him. According to Minor A, Brown had a camera in the Subject Vehicle. Thus, I expect that the Subject Vehicle will contain evidence, fruits, and instrumentalities of the Subject Offenses.

79. On January 23, 2013, Supervisory Special Agent Mark Karengekis sent Facebook a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Subject Facebook Account for 90 days.

80. On January 23, 2013, Supervisory Special Agent Mark Karengekis sent Microsoft a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Subject MSN Account for 90 days.

81. On January 23,,2013, Supervisory Special Agent Mark Karengekis sent Yahoo! a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Subject Yahoo! Account for 90 days.

82. On January 30, 2013, Supervisory Special Agent Mark Karengekis sent Google a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Subject Gmail Account for 90 days.

83. On January 30, 2013, Supervisory Special Agent Mark Karengekis sent Skype a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Subject Skype Account for 90 days.

TECHNICAL BACKGROUND ON FACEBOOK

84. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

85. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth

date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

86. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

87. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

88. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming

"events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

89. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

90. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

91. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

92. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized

message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

93. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

94. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

95. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

96. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a

Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

97. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

98. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

TECHNICAL BACKGROUND ON

YAHOO.COM, GMAIL.COM, AND MSN.COM ACCOUNTS

99. In my training and experience and through discussions with other agents, I have learned that e-mail hosting companies, such as Yahoo, Google, Microsoft, maintain computer servers connected to the Internet. Their customers use those computers to send e-mail on the Internet

100. Customers can access their accounts on the company's e-mail servers from any computer connected to the Internet.

101. When an e-mail user sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the computer servers of the user's e-mail provider, and then transmitted to its end destination. Conversely, an e-mail sent to an e-mail recipient resides on the computer servers of the recipient's e-mail provider until it is transferred by the recipient to his computer to be read.

102. In addition, these companies have storage capacity that allows customers to store opened incoming mail and sent mail indefinitely if they choose, subject to a maximum size limit.

103. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

104. Some e-mail providers can also provide the following additional information associated with a subscriber's account: address books; buddy lists; photos, files, data, or other information; and World-Wide Web profiles or homepages.

105. According to the Yahoo! website (http://messenger.yahoo.com/features), a Yahoo! Inc. subscriber has access to a number of features when using Yahoo! Messenger, an instant messaging service available to subscribers. These features include, but are not limited to, "Photo Sharing: Share photos from your desktop or Flickr, then discuss them over IM while you and a friend view them together," and "Webcam: Plug in your webcam to share live video with your friends on Yahoo! Messenger."

106. The *Compliance Guide For Law Enforcement*, published by Yahoo! Inc., states that "Yahoo! now offers unlimited storage for its free mail services." The *Compliance Guide* also lists some of the information that is or may be available by way of valid process served on Yahoo! Inc. According to Yahoo! Inc., this information includes, but is not limited to:

a. Subscriber Information

   i. Subscriber information supplied by the user at the time of registration, including name, location, date account created, and services used.

   ii. IP addresses associated with log-ins to a user account are available for up to one year.

   iii. Registration IP address data available for IDs registered since 1999.

b. Yahoo! Mail (including email associated with specific properties such as Personals, Small Business, Domains, and Flickr)

   i. Any email available in the user's mail account, including IP address of computer used to send email.

   ii. Yahoo! is not able to search for or produce deleted emails.

   iii. Note that Yahoo! now hosts two new email domains: ymail.com and rocketmail.com.

c. Yahoo! Chat/Messenger

   i. Friends List for Yahoo! Messenger.

   ii. Time, date, and IP address logs for Chat and Messenger use within the prior 45-60 days.

iii. Archives of Messenger communications may be available on the user's computer if the user has chosen to archive communications.

iv. Archives of Web Messenger communications may be stored on Yahoo! servers if at least one party to the communication chose to archive communications.

d. Yahoo! Groups

i. Member list, email addresses of members, and date when members joined the Group.

ii. Information about Group moderators.

iii. Contents of the Files, Photos, and Messages sections.

iv. Group activity log describing when members subscribe and unsubscribe, post or delete files, and similar events.

v. Note: Message Archive does not contain attachments to messages.

e. Yahoo! Flickr

i. Contents in Flickr account and comments on other users' photos.

ii. IP address and timestamp of content uploaded to account.

iii. Flickr Groups to which a user belongs and Group content.

f. Yahoo! Profiles

i. Contents of a user's profile.

ii. Time, date, and IP address logs of content added.

TECHNICAL BACKGROUND ON SKYPE

107. Skype is an online communications service provider that enables users to use various devices that have the Skype application, including a cell phone, computer or a television, to speak, see, and instant message with other Skype users. For a fee, users can call phones, access WiFi or send texts.

108. In response to a subpoena, warrant, or other court order, Skype can provide a user's registration details (i.e., information captured at the time of account registration and current e-mail address), billing address, a list of SkypeIn numbers currently subscribed to be a user, financial transactions conducted with Skype, historical call detail records for calls placed to and from public switched telephone network, SMS text message historical detail records, historical Skype Wi-Fi records, and historical e-mail and password change activity.

LEGAL AUTHORITY

109. The government may obtain both electronic communications and subscriber information from an online communications service provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

110. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

111. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER(S)

112. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise. I further request that, pursuant to 18 U.S.C. § 2705(b), the Court order Facebook, Microsoft, Yahoo, and Google, not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, or the execution of the warrant unless and until authorized to do so by the Court. Such an order is justified because notification of the application, the warrant, or the execution of the warrant could seriously jeopardize the ongoing investigation by giving the subscriber an opportunity to destroy evidence, notify confederates, or flee from prosecution.

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

113. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Facebook, Microsoft, Yahoo, and Google, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g),[1] and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

114. Based on the training and experience of myself and other law enforcement, I understand that online communications service providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that online communications service providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

115. The United States does not ask for this extra data or participate in its production.

116. Should Facebook or Microsoft produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Facebook or Microsoft,

[1] Section 2703(g) provides that "[n]otwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service." 18 U.S.C. § 2703(g).

including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s) absent a follow-up warrant.

117. For these reasons, I request that the Court approve the procedures in Attachment B, which set forth these limitations.

SEARCH & SEIZURE OF COMPUTER EQUIPMENT AND DATA

118. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e mail, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online. I am also aware that the Consumer Electronics Association estimated that in 2010, 86 percent of all U.S. households owned at least one computer.

119. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user generated files, computer storage media – in particular, computers' internal hard drives - contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

120. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media ("computer equipment") be seized and subsequently processed by a qualified computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence C storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.

b. Technical requirements - analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis

protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, password protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

c. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere. If agents believe that the computer equipment may contain child pornography (i.e., contraband), they will seize the computer equipment for subsequent processing.

121. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize them onsite or off-site in order to determine their true use or contents, regardless of how their contents or ownership appear or are described by others at the scene of the search.

CONCLUSION

122. Based on the information described above, I have probable cause to believe that between December 23, 2012 and January 19, 2013, Brown committed the Subject Offenses.

123. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses, as described in Attachment B, are contained within the subject accounts, premises, and items described in Attachment A.

124. Based on the information described above, I have probable cause to believe that on or about January 8, 2013, the defendant committed a violation of Title 18, United States Code, Section 2251, to wit, the defendant did employ, use, persuade, induce, and entice Minor A to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct and for the purpose of transmitting a live visual depiction of such conduct, and the defendant did know and have reason to know that such visual depiction will be transported or transmitted using a means and facility of interstate commerce and in and affecting interstate commerce, and that the visual depiction was produced and transmitted using materials that have been mailed, shipped, or transported in and affecting interstate commerce by any means, including by computer, and that the visual depiction has actually been transported and transmitted using a means and facility of interstate commerce and in and affecting interstate.

Sworn to under the pains and penalties of perjury,

Ian D. Smythe
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 31, 2013

HONORABLE KENNETH P. NEIMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE PROPERTY TO BE SEARCHED

1. The Subject Facebook Account includes information associated with the following user and/or Facebook user ID and that is stored at premises owned, maintained, controlled, or operated by Facebook:

Subject: Ronald S. Brown

E-mails: energizer2758@yahoo.com, rabbit2758@gmail.com, and rabbit2758@msn.com

FaceBook User ID: Ronnie.brown01267

This information is maintained by Facebook, which accepts service of process at:

Facebook, Inc.,
Security Department/Custodian of Records
156 University Avenue, Palo Alto, CA 94301
Fax: 650-644-3229

2. The Subject Yahoo Account is (1) energizer2758@yahoo.com, (2) other user-generated data stored with this account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Yahoo, which accepts service of process at:

Yahoo! Inc.
Custodian of Records
Attn: Compliance Team,
701 First Avenue, Sunnyvale, CA 94089,
Fax : 408-349-7941

3. The Subject Gmail Account is (1) rabbit2758@gmail.com, (2) other user-generated data stored with this account, and (3) associated subscriber, transactional, user connection

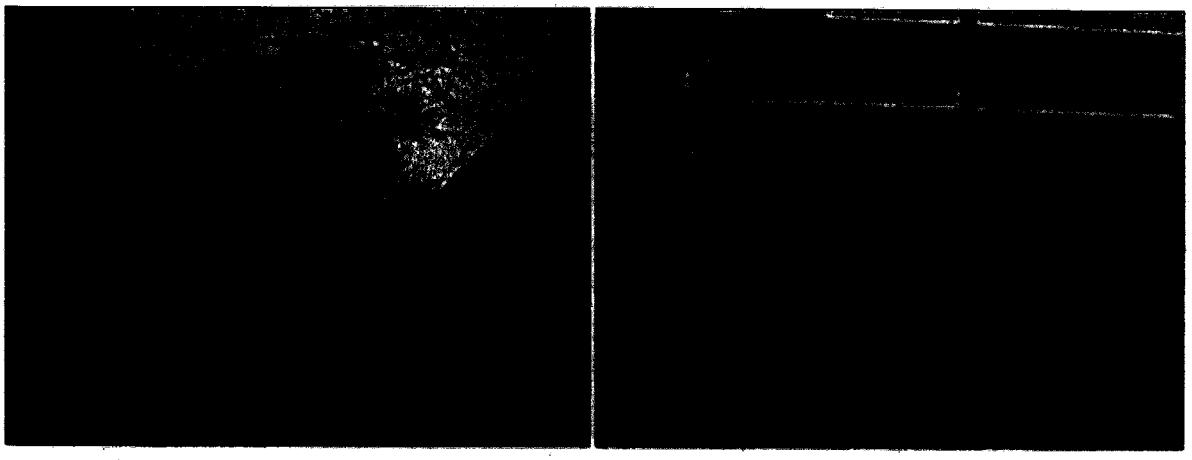
information associated with the account, as described further in Attachment B. This information is maintained by Google, which accepts service of process at:

Google, Inc.
Attention: Custodian of Records
1600 Amphitheatre Parkway
Mountain View, CA 94043
Fax: 650-649-2939

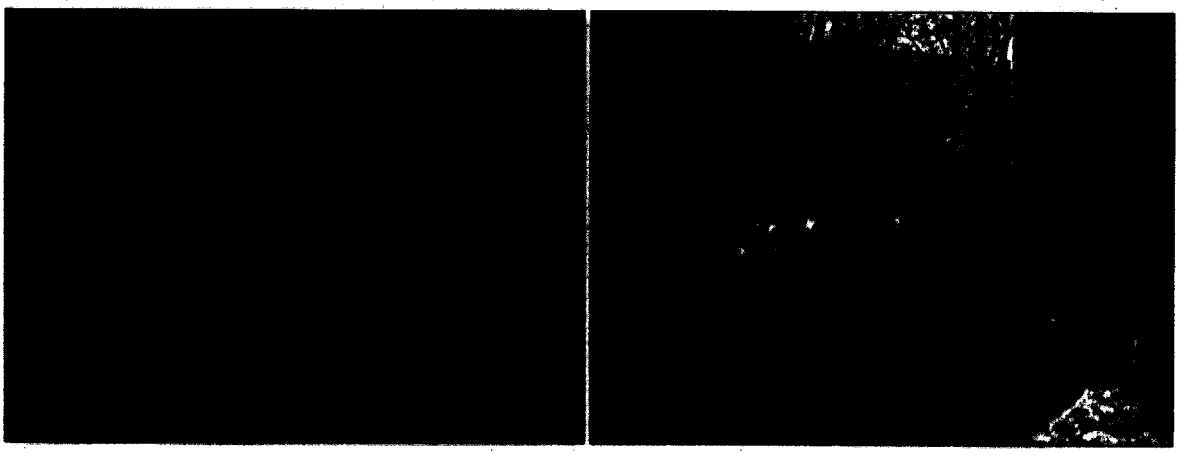
4. The Subject MSN Account is (1) rabbit2758@msn.com, (2) other user-generated data stored with this account, and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Microsoft, which accepts service of process at:

Microsoft Corporation
Attn: MSN Custodian of Records
One Microsoft Way, Redmond, WA 98052
Fax: 425-727-3490

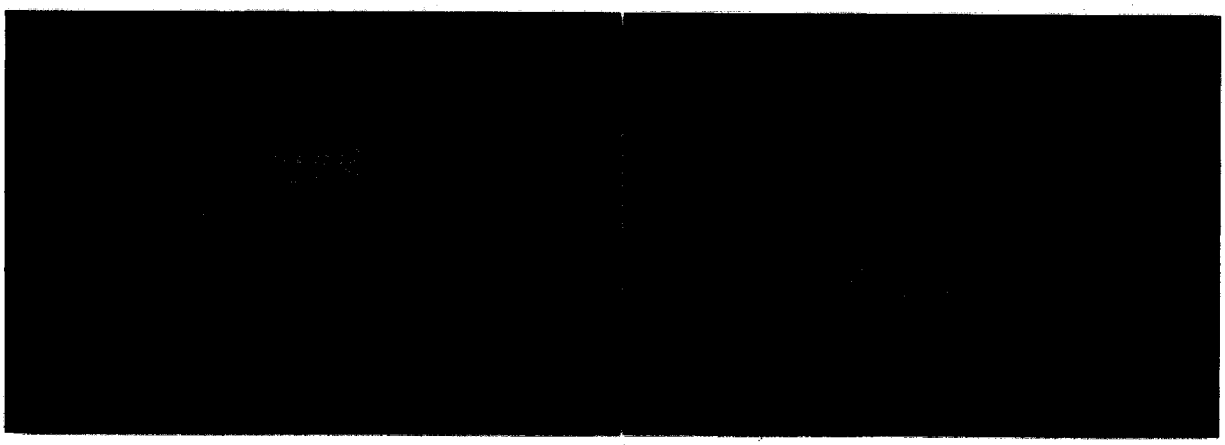
5. The Subject Residence is the residence of Ronald S. Brown, located at , Williamstown, Massachusetts, including any garages, sheds, and outbuildings. The residence is pictured below and is further described as a standalone, two-story, multi-family dwelling, yellow in color with blue trim. Apartment is accessed through the rightmost of two doors to the streetside of the residence that leads to an enclosed porch area from which the apartment is accessed.



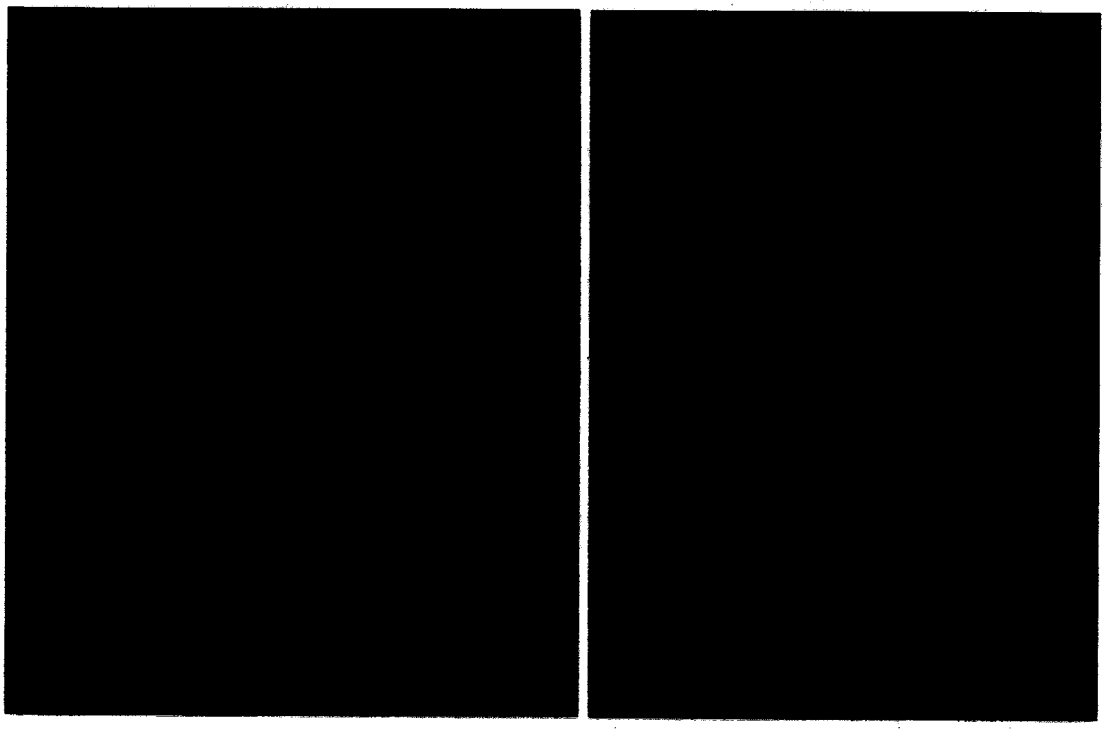
6. The Subject Vehicle is a blue, 2008, four-door Dodge Ram Quad Cab Pickup with MA license plate No. 69YN86 (pictured below).



7. The Subject Laptop is a Sony VAIO laptop computer with serial number C6021UER (pictured below).



8. The Subject Cell Phone is a HTC Incredible cellular telephone with serial number HT26J310727 (pictured below).



ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violation of Title 18, United States Code, Sections 2251 (Sexual Exploitation Of Minors), 2252(a)(2) (Receipt Of Material Involving The Sexual Exploitation Of Minors), 2252(a)(4)(B) (Possession Of Material Involving The Sexual Exploitation Of Minors, 2252A(a)(2) (Receipt Of Child Pornography), 2252A(a)(5)(B) (Possession Of Child Pornography), 2422(b) (Enticement Of A Minor To Engage In Criminal Sexual Activity), and 2423(a) (Transportation Of A Minor With Intent To Engage In Criminal Sexual Activity), including those related to:

A. The following topics:

1. Child sexual exploitation

2. Child pornography

3. Child erotica

4. Any communications with (Minor A).

5. Any communications regarding sexually explicit conduct with minors.

B. For any computer hardware, computer software, computer related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of malicious computer software that would allow others to control the computer equipment, computer software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter forensic programs and associated data that are designed to eliminate data;

5. evidence of the times the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and

C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All computer hardware, computer software, computer related documentation, and storage media. Off site searching of these items shall be limited to searching for the items described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If, after inspecting seized computer equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.